u9/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/672,495	09/29/2000	Ernie F. Brickell	PM 271383	2630

27496 7590 01/13/2005

PILLSBURY WINTHROP LLP
725 S. FIGUEROA STREET
SUITE 2800
LOS ANGELES, CA 90017

EXAMINER	
AKPATI, ODAICHE T	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/672,495	**Applicant(s)** BRICKNELL ET AL.	
	Examiner Tracey Akpati	**Art Unit** 2135	

-- Th MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 June 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 March 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-28 are pending. Claim 5 has been cancelled. Claims 1, 6, 9, 14, 17, 20, 21 and 24 are amended.

Response to Arguments

Applicant's arguments filed 6/22/04 have been fully considered but they are not persuasive.

2. *The attorney argues that Jablon teaches that only some of the pieces of the private key U are stored on different machines, which is not the same as storing each piece of the plurality of pieced of the password on a different one of a plurality of servers.* Jablon discloses storing each piece of the key (which represents the inventor's password) on paragraph 83. The blinded/encrypted share of the user's master key is retrieved from each server from where it was stored. The blinded share represents an encrypted key share.

3. *The attorney argues that Jablon does not teach a method that includes "deleting the password and the plurality of pieces of the password from the client."* This limitation is a new limitation and is rejected as shown below.

4. *The attorney argues that Jablon does not meet the limitation of "receiving an encrypted portion of the password, the encrypted portion of the password comprising less than the entire password."* The limitation is disclosed by Jablon on paragraph 82. The referenced paragraph discloses the master symmetric key, Km where each ith share Si is formed as a function of her password P raised to a random exponent yi. Hence these shares are encrypted because the

reference discloses that the shares are combined with a function so that it can be indistinguishable to an attacker.

5. *With respect to Claim 6, the attorney argues that Jablon does not disclose "storing the encrypted portion of the password with identification information for a user of the encrypted portion of the password."* This limitation is met by Jablon on paragraph 83. This is because in this referenced paragraph it states that Alice sends a randomly blinded/encrypted form of the password Q to each server, each server in turn responds with a blinded reply, Ri consisting of the blinded/encrypted password raised to power of the secret exponent value which represents a blinded/encrypted share of the user's master key. Hence it would have been obvious to store each share at each server. This is because each server will eventually generate each share necessary to constitute the original master key/password. Jablon therefore provides a more secure way of achieving the same results as the applicant's invention.

6. *With respect to Claim 10, the attorney argues that Jablon does not meet the limitation of "receiving an encrypted version of a portion of the first password from each of the plurality of servers at which the authentication was successful, each of the portions of the first password containing less than the entire password."* This limitation is met by Jablon on paragraph 83 and 85. The reasoning behind this has already been discussed above. The authentication process is disclosed by paragraph 85 and 92.

7. With respect to Claim 10, the limitation of "decrypting the received encrypted portions of the first password using encryption keys based on the second password" is sufficiently met by Jablon on paragraph 85, 283. Alice unblinds/decrypts each reply (on paragraph 85) to obtain each key share which is used to rebuild the master key.

8. With respect to Claim 14, the limitation has been newly amended. This new limitation is rejected as shown below, and hence the attorney's arguments are moot.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon (US2002/0067832 A1).

With respect to Claim 1, the limitation of "dividing the password received from a client into a plurality of pieces" on paragraph 20; and "storing each piece of the plurality of pieces of the password on a different one of a plurality of servers, each of the plurality of servers being independent from others of the plurality of servers" on paragraphs 63,79; and "separately authenticating a user at each of the plurality of servers, each of the plurality of servers transmitting the piece of the password stored at the respective server to the user when the authentication at that server is successful" on paragraphs 85, 92; and "assembling the password from the password pieces transmitted from the plurality of servers" is met on paragraphs 63, 85. The limitation of "deleting the password and the plurality of pieces of the password from the client" is met on paragraph 147. Jablon does not explicitly show storing each piece of the password on a different server but however suggests (on paragraph 83) storing exponent yi, U_k and $proof_{PKM}$ on each server that is used, when needed, to generate each share at each given server. Hence instead of storing the shares, its components are stored by each server and will be used for its generation when need be. This achieves the same results as the applicant's invention and instead provides a more secure way of storing shares at each server. Deleting the password or pieces of the password from the server after use is obvious so as not to allow an intruder to gain access to the secure password.

It would have been obvious to one of ordinary skill in the art at the time of the invention to store the shares at each server based on Jablon's disclosure because saving the shares directly on each server, even though less secure, saves processing time needed to compute each share and hence generates the original master key/password in less time.

With respect to Claim 2, 7, 18 and 22, the limitation of "wherein the password is a private key in a public/private key pair" is met on paragraph 82.

With respect to Claim 3, the limitation of "wherein a second password is used to authenticate the user at each of the plurality of servers, the second password being a weak password" is met on paragraph 280 and 282. In the reference the weak password is represented by the PIN code.

With respect to Claim 4, the limitation of "wherein each of the pieces of the password are encrypted before being stored on each of the servers, encryption keys for the encryption of the password pieces being derived from the second password" is met on paragraphs 280 and 282.

With respect to Claim 6 and 21 the limitation of "receiving an encrypted portion of the password, the encrypted portion of the password comprising less than the entire password; storing the encrypted portion of the password with identification information for a user of the encrypted portion of the password" is met on paragraph 82 and 83; and "receiving a request for the encrypted portion of the password, the request including the identification information" is met on paragraph 83; and "returning the encrypted portion of the password to the user when the identification information in the request matches the stored identification information" is met on paragraphs 83 and 85.

With respect to Claim 8, 19, 23, the limitation of "wherein the received encrypted portion of the password is encrypted based on a symmetric encryption of the portion of the password using a key based on a second 'password, the second password being a weak password" is met on paragraph 82.

With respect to Claim 9, 20, 24, the limitation of "wherein the identification information of the user of the encrypted portion of the password is based on the second password" is met on paragraphs 280-283.

With respect to Claim 10, the limitation of "entering a second password of the user; and authenticating the user at each of a plurality of servers based on the second password, the plurality of servers being independent from one another" is met on paragraph 282; and "receiving an encrypted version of a portion of the first password from each of the plurality of servers at which the authentication was successful, each of the portions of the first password containing less than the entire password decrypting the received encrypted portions of the first password using encryption keys based on the second password" is met on paragraphs 83, 85 and 283; and "assembling the first password from the decrypted portions" is met on paragraph 283.

With respect to Claim 11 and 26, the limitation of "wherein the first password is a strong user password" is met on paragraph 79.

With respect to Claim 12 and 27, the limitation of "wherein the first password is a private key in a public/private key pair" is met on paragraph 82.

With respect to Claim 13 and 28, the limitation of "wherein the second password is a weak password" is met on paragraph 280 and 282.

With respect to Claim 14, the limitation of "dividing a password entered by the user into a plurality of pieces" is met on paragraph 20; and "transmitting each piece of the plurality of pieces to corresponding ones of a plurality of remote servers, each of the plurality of remote servers being independent from others of the plurality of remote servers, and each of the remote servers having a respective piece of the plurality of pieces of the password pre-registered with the remote server" is met on paragraph 82; and "comparing the transmitted piece of the plurality of pieces of the password to the pre-registered piece of the password at the plurality of servers" is met on paragraph 83-85; and "generating an authentication accept message at each of the plurality of servers at which the pre-registered piece of the password matches the transmitted piece of the plurality of pieces of the password" on paragraph 86; and "authenticating the user when the authentication accept message is generated for all of the plurality of pieces of the password at the plurality of servers" is met on paragraph 86-87.

With respect to Claim 15, the limitation of "wherein a piece of the password is pre-registered at a computer local to the user and the authentication accept message is generated by the computer local to the user when the pre-registered piece of the password at the computer local to the user matches a corresponding piece of the password entered by the user" is met on paragraph 85-86.

With respect to Claim 16, the limitation "wherein the authentication accept messages are received and accepted at a content server remote from the user" is met inherently on paragraph 86.

With respect to Claim 17, the limitation of "a computer memory" is met inherently on paragraph 63; and "a processor coupled to the computer memory, the processor" inherently on paragraph 63. The limitation of "the processor receiving an encrypted portion of a password, the encrypted portion of the password comprising less than the entire password; storing over a secure connection the encrypted portion with identification information of a user of the encrypted portion of the password; receiving a request for the encrypted portion of the password, the request including the identification information; and returning the encrypted portion of the password to the user when the identification information in the request matches the stored identification information" is similar to Claim 6 limitation and hence its rejection can be found therein.

The limitation of "wherein the computer server is independent of other computer servers storing other portions of the password" is met on Fig. 1.

With respect to Claim 25, the limitation of "receiving a second password entered by the user" is met on paragraph 280; and "authenticating the user at each of a plurality of servers based on the second password, the plurality of servers being independent from one another" is met on paragraph 280 and 282; and "receiving an encrypted version of a portion of the first password from each of the plurality of servers at which the authentication was successful, each of the portions of the first password containing less than the entire password" is met on paragraph 283; and "decrypting the received encrypted portions of the first password using encryption keys based on the second password" is met on paragraph 283; and "assembling the first password from the decrypted portions" is inherently on paragraph 283.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 571-272-3846. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KIM VU
SUPERVISORY PATENT EXA
TECHNOLOGY CENTER 2